# AN ARCHIMEDIAN ANALOG OF IWASAWA THEORY

KEN-ICHI SUGIYAMA,

Abstract. We will show a conjecture which reduces Mazur-Tate-Teitelbaum conjecture to the known cases. In order to explain its background we will develop an archimedian analog of Iwasawa theory. Moreover consequences of the conjecture which are related to Birch and Swinnerton-Dyer conjecture will be discussed. AMS classification 2000: 11F11, 11F67, 11F85, 11G05, 11G40

## 1. Introduction

In this report we will describe a conjecture which reduces Mazur-Tate-Teitelbaum conjecture (see **Conjecture 3.1**) to the known cases. We fix a prime $p$ greater than or equal to 5. Let $E$ and $E'$ be elliptic curves defined over $\mathbb{Q}$. We say that they have ordinary reduction of the same type at $p$ if one of the following conditions holds:

(1) they have good ordinary reduction at $p$ and the cardinality of $\mathbb{F}_p$-rational points of their reductions are equal,
(2) they have split multiplicative reduction at $p$,
(3) they have non-split multiplicative reduction at $p$.

In particular if $E$ has ordinary reduction at $p$ and if their reduction $\tilde{E}_p$ and $\tilde{E}'_p$ are isomorphic over $\mathbb{F}_p$ they have the same type.

**Conjecture 1.1.** *Let $E$ and $E'$ be elliptic curves defined over $\mathbb{Q}$. Suppose that they have ordinary reduction of the same type at $p$. Then*

$$\mathrm{ord}_{s=1}L(E,s) - \mathrm{ord}_{s=0}\mathcal{L}_{E,p}(s) = \mathrm{ord}_{s=1}L(E',s) - \mathrm{ord}_{s=0}\mathcal{L}_{E',p}(s).$$

It is clear that Mazur-Tate-Teitelbaum conjecture implies **Conjecture 1.1**. Conversely we will show that **Conjecture 1.1** indues theirs. Here is a brief outline of an argument (see \$3.1 for details). It is known that Mazur-Tate-Teitelbaum conjecture is true for an elliptic curve $E$ defined over $\mathbb{Q}$ whose L-function does not vanish at $s = 1$. More precisely if $E$ has a good ordinary or a non-split multiplicative reduction at $p$ it is obviously true by the definition (see **Fact 2.1**). If $E$ has a split multiplicative reduction it is a theorem due to Greenberg-Stevens [2] (see also [5]). Suppose that our conjecture were true. It is sufficient to find an elliptic curve $E'$ defined over $\mathbb{Q}$ which has an ordinary reduction of the same type at $p$ as $E$ and that $L(E', 1) \neq 0$. Using results of Ono and Skinner [8] we will

Research supported by in part by JSPS grants Kiban(C)22540068

Address : Chiba University, Yayoi-cho Inage-ku, Chiba, Japan
E-mail address : sugiyama@math.s.chiba-u.ac.jp .

construct such a curve by a quadratic twist of $E$.

Let us briefly explain a motivation of the conjecture. Let $\Gamma_\infty$ be the set of $p$-adic integers congruent one modulo $p$. For an elliptic curve defined over $\mathbb{Q}$ which has ordinary reduction at $p$, Mazur, Tate and Teitelbaum constructed an element $\mu_{E,p} \in \mathbb{Z}_p[[\Gamma_\infty]]$ which interpolates special values of twisted L-function of $E$ at $s = 1$ (see **Fact 2.1**). The $p$-adic L-function of $E$ is intuitively

$$\mathcal{L}_{E,p} = \chi_s(\mu_{E,p}),$$

where $\chi_s$ is a character of $\Gamma_\infty$ defined by $\chi_s(x) = x^{-s}$. Let $E$ and $E'$ be elliptic curves defined over $\mathbb{Q}$ which have ordinary reduction of the same type at $p$ and $\chi$ a character of $\Gamma_\infty$ of finite order. Then

$$\sigma(\chi(\phi(\mu_{E,p})))\frac{L(E', \chi^{1-p}, 1)}{\Omega_{E'}} = \sigma(\chi(\phi(\mu_{E',p})))\frac{L(E, \chi^{1-p}, 1)}{\Omega_E},$$

where $\phi$ is a homomorphism of $\mathbb{Z}_p[[\Gamma_\infty]]$ induced by an automorphism $x \mapsto x^{p-1}$ $(x \in \Gamma_\infty)$ and $\sigma$ is an isomorphism from $\mathbb{C}_p$ to $\mathbb{C}$. Suppose we were able to constructed a $\mathbb{C}$-valued measure $\xi_{\infty,E}$ and $\xi_{\infty,E'}$ on $\Gamma_\infty$ satisfying

(1) $\chi(\xi_{\infty,E}) = L(E, \chi^{1-p}, 1)$ for a finite character of $\Gamma_\infty$,
(2) $\chi_s(\xi_{\infty,E}) = L(E, 1 + (1-p)s)$,

and so does $\xi_{\infty,E'}$. If we brutely replace $\chi$ in the above equation by $\chi_s$ we will obtain

$$\sigma(\mathcal{L}_{E,p}((p-1)s))\frac{L(E', 1 + (1-p)s)}{\Omega_{E'}} = \sigma(\mathcal{L}_{E',p}((p-1)s))\frac{L(E, 1 + (1-p)s)}{\Omega_E},$$

which implies **Conjecture 1.1**. In order to realize this idea we will develop a $\mathbb{C}$-valued measure theory on $\Gamma_\infty$ for an elliptic curve in \$2.2 and \$2.3, which is an arichmedian analog of Iwasawa theory. The motivation will be explained in \$2.4. (Note that the naively conjectured this equation is seemed to be too strong. In fact if $E$ and $E'$ has a split multiplicative reduction at $p$ and if their L-functions does not vanish at $s = 1$ it says that their L-invariants should be equal. But this fact is true if $E'$ is a quadratic twist of $E$, which we may impose to derive consequences from **Conjecture 1.1**.) In \$3.1 we will discuss a relation between **Conjecture 1.1** and the conjecture of Mazur-Tate-Teitelbaum. The remaining sections will be devoted to an application to Birch and Swinnerton-Dyer conjecture.

Throughout the paper we will use the following notation. $p$ will be a prime greater than or equal to 5. Let $G$ be a group and $K$ be a commutative field. We denote the group ring of $G$ whose coefficients are in $K$ by $K[G]$. Fixing an embedding we will consider $\bar{\mathbb{Q}}$ as a subfield of $\mathbb{C}$ and $\mathbb{C}_p$.

## 2. A motivation of the conjecture

2.1. **Review of the theory of $p$-adic measures.** In this section we will review the theory of $p$-adic integrals and $p$-adic L-functions. Details will be found in [3], [6] and [7].

For a positive integer $r$ let $\Gamma_r$ be the kernel of the mod $p$ reduction map,

$$(\mathbb{Z}/(p^{r+1}))^\times \to (\mathbb{Z}/(p))^\times.$$

It is isomorphic to an additive group $\mathbb{Z}/(p^r)$ and taking the inverse limit we have

$$\Gamma_\infty := \varprojlim \Gamma_r \overset{\log}{\simeq} \mathbb{Z}_p.$$

Explicitly $\Gamma_\infty$ is the set of $p$-adic integers congruent to 1 modulo $p$ and

$$\log x = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}(x-1)^n, \quad x \in \Gamma_\infty.$$

The isomorphism between $\Gamma_r$ and $\mathbb{Z}/(p^r)$ is still denoted by log. There is an isomorphism

$$\mathbb{Z}_p[\Gamma_r] \simeq \mathbb{Z}_p[t]/((1+t)^{p^r}-1), \tag{1}$$

defined by

$$\varphi = \sum_{x \in \Gamma_r} \varphi(x)x \mapsto \sum_{x \in \Gamma_r} \varphi(x)(1+t)^{\log x}.$$

Let $\gamma \in \Gamma_\infty$ be a topological generator so that $\log \gamma = 1$. Taking the inverse limit of (1) we have

$$\mathbb{Z}_p[[\Gamma_\infty]] := \varprojlim \mathbb{Z}_p[\Gamma_r] \overset{\varpi_p}{\simeq} \mathbb{Z}_p[[t]], \quad \varpi_p(\gamma) = 1 + t.$$

Via $\varpi_p$ we sometimes identfy $t$ with $\gamma - 1$. Putting

$$t = e^{-s} - 1 = \sum_{n=1}^{\infty} \frac{(-s)^n}{n!},$$

$\varpi_p$ yields an injective homomorphism of $\mathbb{C}_p$-algebras:

$$\Lambda_{\mathbb{C}_p} := \mathbb{Z}_p[[\Gamma_\infty]] \otimes_{\mathbb{Z}_p} \mathbb{C}_p \overset{\tau_p}{\hookrightarrow} \mathbb{C}_p[[s]], \quad \tau_p(\gamma) = \sum_{n=0}^{\infty} \frac{(-s)^n}{n!}. \tag{2}$$

More explicitly using $p$-adic integral

$$\tau_p(\mu)(s) = \sum_{n=0}^{\infty} \frac{(-s)^n}{n!} \int_{\Gamma_\infty} (\log x)^n d\mu(x), \quad \mu \in \Lambda_{\mathbb{C}_p}. \tag{3}$$

Let $a$ $(\neq 1)$ be a $p$-adic integer that is congruent 1 modulo $p$. We define *a Dirac measure* $\delta_a$ supported at $a$ to be

$$\delta_a := \varprojlim (\delta_a)_r \in \mathbb{Z}_p[[\Gamma_\infty]], \quad (\delta_a)_r = \sum_{x \in \Gamma_r} (\delta_a)_r(x)x \in \mathbb{Z}_p[\Gamma_r],$$

where $(\delta_a)_r([a]) = 1$ and $(\delta_a)_r(x) = 0$ if $x \neq [a]$. Here $[a]$ is the image of $a$ by the natural projection $\Gamma_\infty \to \Gamma_r$. A simple computation shows the following lemma.

**Lemma 2.1.**

$$\tau_p(\delta_a)(s) = a^{-s}.$$

*where*

$$a^{-s} := \sum_{n=0}^{\infty} \frac{(-s \log a)^n}{n!} \in \mathbb{C}_p[[s]].$$

For an example let us take $a = \gamma$. Then (1) is a consequentce of (2). Let $\mathbb{C}_p[\delta_a]$ be a subalgebra of $\Lambda_{\mathbb{C}_p}$ generated by $\delta_a$, which is easily seen to be isomorphic to a ring of polynomials of one variable whose coefficients are in $\mathbb{C}_p$. In fact let us consider a sub-semigroup $a^{\mathbb{N}} := \{a^m \,|\, m \in \mathbb{Z},\, m \geq 0\}$ of $\Gamma_\infty$ which is isomorphic to $\mathbb{N} := \{x \in \mathbb{Z} |\, x \geq 0\}$. Then

$$\mathbb{C}_p[\delta_a] = \mathbb{C}_p[a^{\mathbb{N}}] \subset \Lambda_{\mathbb{C}_p}.$$

We put $X_a = \delta_a - 1$ and define

$$\mathfrak{M}_p := \tau_p^{-1}((s)), \quad \mathfrak{N} := \mathfrak{M}_p \cap \mathbb{C}_p[X_a].$$

Then $\mathfrak{M}_p$ and $\mathfrak{N}$ are generated by $t$ and $X_a$, respectively. Let $\mathbb{C}_p[[X_a]]$ (resp. $\hat{\Lambda}_{\mathbb{C}_p}$) be a $\mathfrak{N}$-adic (resp. $\mathfrak{M}_p$-adic) completion of $\mathbb{C}_p[X_a]$ (resp. $\Lambda_{\mathbb{C}_p}$). Note that

$$\mathbb{C}_p[X_a]/(X_a^r) = \Lambda_{\mathbb{C}_p}/\mathfrak{M}_p^r \overset{\tau_p}{\simeq} \mathbb{C}_p[s]/(s^r), \tag{4}$$

for every positive integer $r$. Passing to the inverse limit we see that

$$\mathbb{C}_p[[X_a]] = \hat{\Lambda}_{\mathbb{C}_p},$$

and that $\tau_p$ is completed to an isomorphism:

$$\mathbb{C}_p[[X_a]] = \hat{\Lambda}_{\mathbb{C}_p} \overset{\hat{\tau}_p}{\simeq} \mathbb{C}_p[[s]].$$

Summarizing we have proved the following.

**Proposition 2.1.** *Let $a$ be an integer greater than 1 that is congruent to 1 modulo $p$.*

(1)
$$\hat{\Lambda}_{\mathbb{C}_p} = \mathbb{C}_p[[X_a]], \quad X_a = \delta_a - 1.$$

(2) *There is an injective homomorphism $\Lambda_{\mathbb{C}_p} \overset{\tau_p}{\hookrightarrow} \mathbb{C}_p[[s]]$ and it is completed to an isomorphism*
$$\mathbb{C}_p[[X_a]] = \hat{\Lambda}_{\mathbb{C}_p} \overset{\hat{\tau}_p}{\simeq} \mathbb{C}_p[[s]], \quad \hat{\tau}_p(X_a) = a^{-s} - 1.$$
*In particular the natural map*
$$\nu : \Lambda_{\mathbb{C}_p} \to \hat{\Lambda}_{\mathbb{C}_p},$$
*is injective.*

Let $\mathbb{C}_p[[\Gamma_\infty]]$ be the inverse limit of a projective system $\{\mathbb{C}_p[\Gamma_r]\}_r$, which contains $\Lambda_{\mathbb{C}_p}$ as a subalgebra. Let $\alpha_{\Gamma_r} : \mathbb{C}_p[\Gamma_r] \to \mathbb{C}_p$ be the argumentation and

$$\alpha_{\Gamma_\infty} : \mathbb{C}_p[[\Gamma_\infty]] \to \mathbb{C}_p,$$

be its inverse limit. Let $e_0 : \mathbb{C}_p[[s]] \to \mathbb{C}_p$ be the evaluation at the origin: $e_0(f) = f(0)$. The following is derived from (3).

**Lemma 2.2.**

$$e_0(\tau_p(\mu)) = \alpha_{\Gamma_\infty}(\mu), \quad \mu \in \Lambda_{\mathbb{C}_p}.$$

This shows that $\mathfrak{M}_p$ is equal to the intersection of $\Lambda_{\mathbb{C}_p}$ with the argumentation ideal of $\mathbb{C}_p[[\Gamma_\infty]]$. We take a system of primitive $p^n$-th roots of the unit $\{\zeta_{p^n}\}_n$ satisfying $\zeta_{p^{n+1}}^p = \zeta_{p^n}$. According to a decomposition of Galois group:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}) \simeq (\mathbb{Z}/(p))^\times \times \Gamma_n,$$

let $\mathbb{Q}_n$ be the abelian extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_{p^{n+1}})$ such that $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \Gamma_n$ and $\mathbb{Q}_\infty$ their union: $\mathbb{Q}_\infty := \cup_n \mathbb{Q}_n$. Then $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ is isomorphic to $\Gamma_\infty$ and we will identify them. Then As we have explained before, the projective limit $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$ of $\{\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})]\}_n$ is isomorphic to $\mathbb{Z}_p[[t]]$.

Let $E$ be an elliptic curve defined over $\mathbb{Q}$ which has either good reduction or multiplicative reduction at $p$. Take a prime $l$ different from $p$ and let $\alpha_E \in \mathbb{Z}_p^\times$ and $\beta_E = p/\alpha_E \in p\mathbb{Z}_p$ be the eigenvalues of the $l$-adic representation of $p$-th power Frobenius on the Tate module $T_l(E)$ if $E$ has good ordinary reduction and $(\alpha_E, \beta_E) = (1, p)$ (resp. $(-1, -p)$) if $E$ has split (resp. non-split) multiplicative reduction at $p$. For a finite character $\chi$ of $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ whose conductor $p^n$ let $W(\chi)$ be the Gauss sum:

$$W(\chi) = \sum_{\gamma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})} \chi(\gamma)\zeta_{p^n}^\gamma.$$

We fix an isomorphism $\sigma : \mathbb{C}_p \simeq \mathbb{C}$ such that

$$\sigma(z) = z, \quad z \in \bar{\mathbb{Q}}.$$

**Fact 2.1.** ([7]) *There is the unique element $\mu_{E,p}$ of $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ satisfying the following properties:*

(1) *If $E$ has good ordinary reduction at $p$,*

$$\sigma(\mathbf{1}(\mu_{E,p})) = (1 - \alpha_E^{-1})^2 \frac{L(E,1)}{\Omega_E}.$$

(2) *If $E$ has multiplicative reduction at $p$,*

$$\sigma(\mathbf{1}(\mu_{E,p})) = (1 - \alpha_E^{-1}) \frac{L(E,1)}{\Omega_E}.$$

(3) *Let $\chi$ be a character of* $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ *of finite order whose conductor $p^n > 1$. Then*

$$\sigma(\chi(\mu_{E,p})) = \frac{W(\chi)}{\alpha_E^n}\frac{L(E,\chi^{-1},1)}{\Omega_E}.$$

Here $\mathbf{1}$ is the trivial character and $\Omega_E$ is the fundamental real period of $E$. The $p$-adic L-function $\mathcal{L}_{E,p}$ of $E$ is defined to be

$$\mathcal{L}_{E,p} := \tau_p(\mu_{E,p}) \in \mathbb{C}_p[[s]].$$

Let $\phi$ and $\iota$ be automorphisms of $\Gamma_\infty$ defined to be

$$\phi(x) = x^{p-1}, \quad \iota(x) = x^{-1}, \quad x \in \Gamma_\infty,$$

and the induced automorphisms on $\Lambda_{\mathbb{C}_p}$ are still denoted by the same character.

**Lemma 2.3.** *Let $\mu \in \Lambda_{\mathbb{C}_p}$.*

(1)
$$\chi(\phi(\mu)) = \chi^{p-1}(\mu), \quad \chi(\iota(\mu)) = \chi^{-1}(\mu).$$

(2)
$$\tau_p(\phi(\mu))(s) = \tau_p(\mu)((p-1)s), \quad \tau_p(\iota(\mu))(s) = \tau_p(\mu)(-s).$$

The following follows from **Fact 2.1** and **Lemma 2.3**

**Proposition 2.2.** (1) *If $E$ has good ordinary reduction at $p$,*

$$\sigma(\mathbf{1}(\iota\phi(\mu_{E,p}))) = (1-\alpha_E^{-1})^2\frac{L(E,1)}{\Omega_E}.$$

(2) *If $E$ has multiplicative reduction at $p$,*

$$\sigma(\mathbf{1}(\iota\phi(\mu_{E,p}))) = (1-\alpha_E^{-1})\frac{L(E,1)}{\Omega_E}.$$

(3) *Let $\chi$ be a character of* $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ *of finite order whose conductor $p^n > 1$. Then*

$$\sigma(\chi(\iota\phi(\mu_{E,p}))) = \frac{W(\chi^{1-p})}{\alpha_E^n}\frac{L(E,\chi^{p-1},1)}{\Omega_E}.$$

(4)
$$\tau_p(\iota\phi(\mu_{E,p}))(s) = \mathcal{L}_{E,p}((1-p)s).$$

2.2. **An archimedian analog of the $p$-adic measure.** We want to develop an analog of the $p$-adic measure theory over $\mathbb{C}$ for a certain Dirichlet series. For $\rho \in \mathbb{R}$ let $H_\rho$ be a right half plane defined by

$$H_\rho := \{z \in \mathbb{C} \,:\, \mathrm{Re}\, z > \rho\}.$$

**Definition 2.1.** *A Dirichlet series*

$$A(z) = \sum_{n=1}^{\infty} a_n n^{-z}, \quad a_n \in \mathbb{C},$$

*will be called* regular *if it satisfies the following conditions:*

(1) *$a_n = 0$ if $p$ divides $n$.*

(2) *There is a positive real number $\rho$ (which may depend on $A(z)$) such that $A(z)$ absolutely converges on $H_\rho$ and is analytically continued to the whole plane as an entire function.*

(3) *For every positive integer $r$ and $a$ such that $1 \leq a \leq p^r$*

$$A_{r,a}(z) := \sum_{k=1, k\equiv a(p^r)}^{\infty} a_k k^{-z}$$

*is also continued to the whole plane as an entire function.*

We will denote the set of regular Dirichlet series by $\mathcal{R}$. By definition it is contained in the commutative algebra $\mathcal{O}_{\mathbb{C}}$ of holomorphic functions on $\mathbb{C}$. In fact it is a subalgebra. We only check that it is closed by a multiplication. Let $A(z) = \sum_{l=1}^{\infty} a_l l^{-z}$ and $B(z) = \sum_{m=1}^{\infty} b_m m^{-z}$ be regular Dirichlet series and $C(z) = \sum_{n=1}^{\infty} c_n n^{-z}$ their product. It is obvious that $C(z)$ satisfies (1) and (2). For $1 \leq c \leq p^r$ a simple computation shows

$$C_{r,c}(z) = \sum_{ab\equiv c(p^r), 1\leq a,b\leq p^r} A_{r,a}(z) B_{r,b}(z), \tag{5}$$

and this implies (3). For $A(z) = \sum_{n=1}^{\infty} a_n n^{-z} \in \mathcal{R}$, we define

$$\mu_{\mathcal{O},r}(A) := \sum_{a=1}^{p^r} A_{r,a}(z)[a]_r \in \mathcal{O}_{\mathbb{C}}[(\mathbb{Z}/(p^r))^{\times}],$$

where $[\cdot]_r$ represents the residue class. Then $\{\mu_{\mathcal{O},r}(A)\}_r$ forms a projective system and we set

$$\mu_{\mathcal{O}}(A) := \varprojlim \mu_{\mathcal{O},r}(A) \in \mathcal{O}_{\mathbb{C}}[[\mathbb{Z}_p^{\times}]].$$

Thus we have a map

$$\mu_{\mathcal{O}} : \mathcal{R} \to \mathcal{O}_{\mathbb{C}}[[\mathbb{Z}_p^{\times}]],$$

which is a homomorphism of algebras by (5). Let $\tilde{\Lambda}_{\mathcal{O}}$ be its image. Note that a regular Dirichlet series $A$ is recovered from $\mu_{\mathcal{O}}(A)$. In fact we associate a function $\sum_{a=1}^{p^r} A_{r,a}(z) a^{-s}$ to $\mu_{\mathcal{O},r}(A)$, that is $\sum_{a=1}^{p^r} \sum_{k=1,k\equiv a(p^r)} a_k k^{-z} a^{-s}$ on $H_\rho \times H_\rho$ ($\rho$ is sufficiently large). Therefore

$$\lim_{r\to\infty} \sum_{a=1}^{p^r} \sum_{k=1,k\equiv a(p^r)} a_k k^{-z} a^{-s} = \sum_{n=1,(n,p)=1}^{\infty} a_n n^{-(s+z)} = A(s+z),$$

on $H_\rho \times H_\rho$ and by analytic continuation we have a map

$$\tilde{\tau}_{\mathcal{O}} : \tilde{\Lambda}_{\mathcal{O}} \to \mathcal{O}_{\mathbb{C}\times\mathbb{C}}, \quad \tilde{\tau}_{\mathcal{O}}(\mu_{\mathcal{O}}(A)) = A(s+z), \tag{6}$$

where $\mathcal{O}_{\mathbb{C}\times\mathbb{C}}$ is the set of holomorphic functions on $\mathbb{C}\times\mathbb{C}$. Thus

$$\tilde{\tau}_{\mathcal{O}} \mu_{\mathcal{O}} = p^*,$$

where

$$p : \mathbb{C}\times\mathbb{C} \to \mathbb{C}, \quad p(s,z) = s+z,$$

and since $p^*$ is an injective homomorphism, $\mathcal{R} \overset{\mu_{\mathcal{O}}}{\to} \tilde{\Lambda}_{\mathcal{O}}$ is an isomorphism and $\tilde{\tau}_{\mathcal{O}}$ is injective. Let

$$e : \mathcal{O}_{\mathbb{C}}[[\mathbb{Z}_p^\times]] \to \mathbb{C}[[\mathbb{Z}_p^\times]],$$

be a homomorphism induced by

$$\mathcal{O}_{\mathbb{C}} \to \mathbb{C}, \quad f \mapsto f(1),$$

and set $\tilde{\tau}_{\mathbb{C}} := \tilde{\tau}_{\mathcal{O}} \otimes_{\mathcal{O},e} \mathbb{C}$. Let $\mu_{\mathbb{C}}$ be the composition of

$$\mathcal{R} \overset{\mu_{\mathcal{O}}}{\simeq} \tilde{\Lambda}_{\mathcal{O}} \overset{e}{\to} \tilde{\Lambda}_{\mathbb{C}}.$$

Then by (6)

$$\tilde{\tau}_{\mathbb{C}} \circ \mu_{\mathbb{C}}(A)(s) = A(1+s), \quad A \in \mathcal{R},$$

and we have proved the following proposition.

**Proposition 2.3.**

$$\mu_{\mathbb{C}} : \mathcal{R} \to \tilde{\Lambda}_{\mathbb{C}},$$

*and*

$$\tilde{\tau}_{\mathbb{C}} : \tilde{\Lambda}_{\mathbb{C}} \to \mathcal{O}_{\mathbb{C}},$$

*are an isomorphism and an injective homomorphism, respectively. Moreover*

$$\tilde{\tau}_{\mathbb{C}}\mu_{\mathbb{C}}(A) = A(1+s), \quad A \in \mathcal{R}.$$

Here is an example. Let $b(\neq 1)$ be a positive integer prime to $p$ and set $D_b := b^{1-z}$, which is a regular Dirichlet series. Then

$$\mu_{\mathbb{C}}(D_b) = \delta_b, \quad \tilde{\tau}_{\mathbb{C}}(D_b) = b^{-s}. \tag{7}$$

Let $\tilde{\tau}_\infty : \tilde{\Lambda}_{\mathbb{C}} \to \mathbb{C}[[s]]$ be the composition of $\tilde{\tau}_{\mathbb{C}}$ with the Taylor expansion at the origin:

$$\mathcal{O}_{\mathbb{C}} \to \mathbb{C}[[s]], \quad f \mapsto \sum_{n=0}^{\infty} a_n(f) s^n,$$

which is injective by **Proposition 2.3**. It is easy to check that

$$\tilde{\tau}_\infty(A)(0) = \alpha_{\tilde{\Lambda}_{\mathbb{C}}}(A), \quad A \in \tilde{\Lambda}_{\mathbb{C}},$$

where $\alpha_{\tilde{\Lambda}_{\mathbb{C}}}$ is the restriction of the argumentation of $\mathbb{C}[[\mathbb{Z}_p^\times]]$. In particular we see that the kernel $\mathfrak{M}_{\tilde{\Lambda}_{\mathbb{C}}}$ of $\alpha_{\tilde{\Lambda}_{\mathbb{C}}}$ is equal to $\tilde{\tau}_\infty^{-1}(s)$. Take a positive integer $b$ as above and set $Y_b := \delta_b - 1$. Then as we have seen in the previous section $\mathbb{C}[Y_b]$ is a subalgebra of $\tilde{\Lambda}_{\mathbb{C}}$ which is isomorphic to the polynomial ring of one variable and it is esy to see that

$$(Y_b) = \mathbb{C}[Y_b] \cap \mathfrak{M}_{\tilde{\Lambda}_{\mathbb{C}}}.$$

Thus we have shown that the each arrow of

$$\mathbb{C}[Y_b]/(Y_b^r) \to \tilde{\Lambda}_{\mathbb{C}}/\mathfrak{M}_{\tilde{\Lambda}_{\mathbb{C}}}^r \overset{\tilde{\tau}_\infty}{\to} \mathbb{C}[[s]]/(s^r) \tag{8}$$

is injective. Since the dimension of both side are equal they are isomorphic. The following is an archimedian analog of **Proposition 2.1**.

**Proposition 2.4.** (1)

$$\mathbb{C}[[Y_b]] = \hat{\tilde{\Lambda}}_{\mathbb{C}} \overset{\hat{\tilde{\tau}}_\infty}{\simeq} \mathbb{C}[[s]].$$

(2) *The natural map* $\tilde{\Lambda}_{\mathbb{C}} \to \hat{\tilde{\Lambda}}_{\mathbb{C}}$ *is injective.*

**Proof.** Take the limit of (8) we obtain (1).

$$\begin{tikzcd}
\mathcal{R} \arrow[r, "\tilde{\tau}_\infty \circ \mu_{\mathbb{C}}"] \arrow[d, "\mu_{\mathbb{C}}"'] & \mathbb{C}[[s]] \arrow[d, "\hat{\tilde{\tau}}_\infty^{-1}"'] \\
\hat{\Lambda}_{\mathbb{C}} \arrow[r] & \hat{\tilde{\Lambda}}_{\mathbb{C}},
\end{tikzcd}$$

Notice that $\tilde{\tau}_\infty \circ \mu_{\mathbb{C}} : \mathcal{R} \to \mathbb{C}[[s]]$ is the Taylor expansion at $s = 1$ and it is injective. Since vertical arrows are isomorphisms we obtain (2).

□

But there is a slight difference. Namely $\Lambda_{\mathbb{C}_p}$ is a subalgebra of $\mathbb{C}_p[[\Gamma_\infty]]$ but $\tilde{\Lambda}_{\mathbb{C}}$ is contained in $\mathbb{C}[[\mathbb{Z}_p^\times]]$. Let

$$\phi : \mathbb{C}[[\mathbb{Z}_p^\times]] \to \mathbb{C}[[\Gamma_\infty]],$$

be a homomorphism induced by

$$\phi : \mathbb{Z}_p^\times \to \Gamma_\infty \quad \phi(x) = x^{p-1},$$

and we define

$$\Lambda_{\mathbb{C}} := \phi(\tilde{\Lambda}_{\mathbb{C}}).$$

Let $\alpha_{\Lambda_{\mathbb{C}}}$ be the restriction of the argumentation of $\mathbb{C}[[\Gamma_\infty]]$ to $\Lambda_{\mathbb{C}}$ and $\mathfrak{M}_\infty$ its kernel. Set $a := b^{p-1}$ and $X_a := \delta_a - 1$. Then $\mathbb{C}[X_a]$ is a subalgebra of $\Lambda_{\mathbb{C}}$ isomorphic to a polynomial ring of one variable and $\phi$ yields a isomorphism:

$$\phi : \mathbb{C}[Y_b] \to \mathbb{C}[X_a], \quad \phi(Y_b) = X_a.$$

Since

$$(X_a) = \mathbb{C}[X_a] \cap \mathfrak{M}_\infty, \quad \phi^{-1}(\mathfrak{M}_\infty) = \mathfrak{M}_{\tilde{\Lambda}_{\mathbb{C}}},$$

we obtain the following diagram.

(9)

$$\begin{tikzcd}
\mathbb{C}[Y_b]/(Y_b^r) \arrow[r, "\tilde{i}"] \arrow[d, "\phi"'] & \tilde{\Lambda}_{\mathbb{C}}/\mathfrak{M}^r_{\tilde{\Lambda}_{\mathbb{C}}} \arrow[r, "\tilde{\tau}_\infty"] \arrow[d, "\phi"'] & \mathbb{C}[[s]]/(s^r) \\
\mathbb{C}[X_a]/(X_a^r) \arrow[r, "i"] & \Lambda_{\mathbb{C}}/\mathfrak{M}^r_\infty &
\end{tikzcd}$$

By (8) upper horizontal arrows are isomorphisms. Since the both $\phi$ are isomorphic so is $i$. (The reason that the right $\phi$ is isomorphic is $\phi : \tilde{\Lambda}_{\mathbb{C}} \to \Lambda_{\mathbb{C}}$ is surjective and $\phi^{-1}(\mathfrak{M}_\infty) = \mathfrak{M}_{\tilde{\Lambda}_{\mathbb{C}}}$.) Define $\hat{\tau}_\infty$ and $\phi$ to be

$$\hat{\tau}_\infty : \mathbb{C}[[X_a]] \to \mathbb{C}[[s]], \quad \hat{\tau}_\infty(X_a) = a^{-s} - 1,$$

and

$$\phi : \mathbb{C}[[s]] \to \mathbb{C}[[s]], \quad \phi(f)(s) = f((p-1)s).$$

Take the limit of (9) and we have

$$\begin{tikzcd}
\tilde{\Lambda}_{\mathbb{C}} \arrow[r, "\tilde{\nu}"] \arrow[d, "\phi"'] & \mathbb{C}[[Y_b]] = \hat{\tilde{\Lambda}}_{\mathbb{C}} \arrow[r, "\hat{\tilde{\tau}}_{\infty}"] \arrow[d, "\phi"'] & \mathbb{C}[[s]] \arrow[d, "\phi"'] \\
\Lambda_{\mathbb{C}} \arrow[r, "\nu"] & \mathbb{C}[[X_a]] = \hat{\Lambda}_{\mathbb{C}} \arrow[r, "\hat{\tau}_{\infty}"] & \mathbb{C}[[s]],
\end{tikzcd}$$

where $\tilde{\nu}$ and $\nu$ are natural homomorphisms and every arrow in the right rectangle is an isomorphism. As we have shown in **Proposition 2.4** $\tilde{\nu}$ is injective and by definition the most left $\phi$ is surjective. A diagram chasing shows that $\nu$ is injective and that the most left $\phi$ is also an isomorphism. Let us denote $\tau_{\infty} = \hat{\tau}_{\infty} \circ \nu$. Here is an archimedean analog of **Proposition 2.2**.

**Proposition 2.5.** (1)

$$\mathbb{C}[[X_a]] = \hat{\Lambda}_{\mathbb{C}} \overset{\hat{\tau}_{\infty}}{\simeq} \mathbb{C}[[s]], \quad \hat{\tau}_{\infty}(X_a) = a^{-s} - 1.$$

(2) *The natural map $\nu : \Lambda_{\mathbb{C}} \to \hat{\Lambda}_{\mathbb{C}}$ is injective.*

(3) *For $A \in \mathcal{R}$ $\tau_{\infty}(\phi \circ \mu_{\mathbb{C}}(A))$ is the Taylor expansion of $A(1 + (p-1)s)$ at the origin and*

$$\alpha_{\Lambda_{\mathbb{C}}}(\phi \circ \mu_{\mathbb{C}}(A)) = A(1).$$

2.3. **An archimedean measure of a cusp form.** Let $f = \sum_{n=1}^{\infty} a_n(f) q^n$ be a cusp form of weight 2 and level $N$. Let us fix a positive integer $m$ and for an integer $0 \le a \le m-1$ we put

$$\phi_m^a = f(z + \frac{a}{m}), \quad f_m^a = \sum_{n=1, n \equiv a(m)}^{\infty} a_n(f) q^n.$$

**Lemma 2.4.** *$\{\phi_m^0, \cdots, \phi_m^{m-1}\}$ and $\{f_m^0, \cdots, f_m^{m-1}\}$ span the same vector space over $\mathbb{Q}(\zeta_m)$.*

**Proof.** Putting $\zeta_m = \exp(2\pi i/m)$ a simple computation shows

$$\phi_m^a = \sum_{n=1}^{\infty} a_n(f) q^n \zeta_m^{an} = \sum_{k=0}^{m-1} \zeta_m^{ak} f_m^k.$$

Therefore

$$\begin{pmatrix} \phi_m^0 \\ \vdots \\ \phi_m^{m-1} \end{pmatrix} = A \begin{pmatrix} f_m^0 \\ \vdots \\ f_m^{m-1} \end{pmatrix}$$

where

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \zeta_m & \cdots & \zeta_m^{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_m^{m-1} & \cdots & \zeta_m^{(m-1)^2} \end{pmatrix}.$$

Since $A$ is regular, we obtain the claim. □

Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and $N_E$ its conductor. Since it is modular [1] there is a cusp form $f_E$ of weight 2 and level $N_E$ associated to $E$ and let

$$f_E = \sum_{n=1}^{\infty} a_n(E) q^n, \quad q = \exp(2\pi i z)$$

be the Fourier expansion at $i\infty$. Removing the Euler factor $L_p(E, z)$ at $p$ we define *the modified $L$-function* of $E$ to be

$$L^{\dagger}(E, z) = \sum_{n=1, (n,p)=1}^{\infty} a_n(E) n^{-z}.$$

Since its partial Dirichlet series

$$(L^{\dagger}(E, z))_{r,a} := \sum_{k=1, k \equiv a(p^r)}^{\infty} a_k(E) k^{-z}$$

is a Mellin transform of $(f_E)^a_{p^r}$ **Lemma 2.4** and the cuspidality of $f_E$ imply that $L^{\dagger}(E, z)$ is a regular Dirichlet series. Now we set

$$\mu_{E,\infty} := \mu_{\mathbb{C}}(L^{\dagger}(E, z)) \in \tilde{\Lambda}_{\mathbb{C}}.$$

Let $\chi$ be a character of $\mathbb{Z}_p^{\times}$ of finite order whose conductor is $p^r$. It defines a homomorphism

$$\chi : \mathbb{C}[(\mathbb{Z}/(p^r))^{\times}] \to \mathbb{C},$$

and the composition it with the projection $\mathbb{C}[[\mathbb{Z}_p^{\times}]] \to \mathbb{C}[(\mathbb{Z}/(p^r))^{\times}]$ is still denoted by $\chi$. Then

$$\chi(\mu_{E,\infty}) = L(E, \chi, 1),$$

for a non-trivial $\chi$ and

$$\mathbf{1}(\mu_{E,\infty}) = \alpha_{\Lambda_{\mathbb{C}}}(\mu_{E,\infty}) = L^{\dagger}(E, 1).$$

Thus we see

$$\chi(\phi(\mu_{E,\infty})) = L(E, \chi^{p-1}, 1),$$

by **Lemma 2.3**. **Proposition 2.5** implies the following theorem, which should be compared to **Fact 2.1**.

**Theorem 2.1.** *Let $E$ be an elliptic curve defined over $\mathbb{Q}$. Then $\phi(\mu_{E,\infty}) \in \Lambda_{\mathbb{C}}$ satisfies the following properties.*

(1)

$$\chi(\phi(\mu_{E,\infty})) = L(E, \chi^{p-1}, 1),$$

*for a non-trivial character $\chi$ of $\Gamma_{\infty}$ of finite order.*

(2)

$$\mathbf{1}(\phi(\mu_{E,\infty})) = L^{\dagger}(E, 1) = \frac{L(E, 1)}{L_p(E, 1)}.$$

(3)
$$\tau_\infty(\phi(\mu_{E,\infty}))(s) = L^\dagger(E, 1 + (p-1)s).$$

Our measure is related to Kato's system which will be recalled below. Let $T_p(E)$ and $V_p(E)$ be the Tate module of $E$:

$$T_p(E) = \lim_{\leftarrow} E[p^n], \quad V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

$\mathbb{Q}_{n,p}$ denotes the completion of $\mathbb{Q}_n$ by the unique prime on $p$. Let $H^1_S(\mathbb{Q}_{n,p}, V_p(E)) \subset H^1(\mathbb{Q}_{n,p}, V_p(E))$ be the image of $E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p$ by the Kummer map and $H^1_S(\mathbb{Q}_{n,p}, T_p(E))$ its intersection of with $H^1(\mathbb{Q}_{n,p}, T_p(E))$. For $M = T_p(E)$ or $V_p(E)$ we define

$$H^1_{/S}(\mathbb{Q}_{n,p}, M) = H^1(\mathbb{Q}_{n,p}, M)/H^1_S(\mathbb{Q}_{n,p}, M).$$

Let $\omega_E$ be the canonical invariant differential associated to the minimal Weierstrauss model of $E$. Then there is an isomorphism called *dual exponential map*:

$$\exp^* : H^1_{/S}(\mathbb{Q}_{n,p}, V_p(E)) \tilde{\to} \mathbb{Q}_{n,p}\omega_E.$$

Restrict the composition of $\exp^*$ with

$$\mathbb{Q}_{n,p}\omega_E \tilde{\to} \mathbb{Q}_{n,p}, \quad a\omega_E \mapsto a$$

to $H^1_{/S}(\mathbb{Q}_{n,p}, T_p(E))$ and we obtain a map

$$\exp^*_{\omega_E} : H^1_{/S}(\mathbb{Q}_{n,p}, T_p(E)) \to \mathbb{Q}_{n,p}.$$

**Fact 2.2.** *(*[4], [11] **Corollary 7.2***) For every $n$ there is $c_n \in H^1(\mathbb{Q}_n, T_p(E))$ satisfying following properties.*

(1)
$$\mathrm{Cor}_{n,n+1}(c_{n+1}) = c_n.$$

*where* $\mathrm{Cor}_{n,n+1} : H^1(\mathbb{Q}_{n+1}, T_p(E)) \to H^1(\mathbb{Q}_n, T_p(E))$ *is a corestriction map.*

(2) *Let* $\mathrm{loc}_p^{ram}$ *be the composition of*

$$H^1(\mathbb{Q}_n, T_p(E)) \overset{\mathrm{loc}_p}{\to} H^1(\mathbb{Q}_{n,p}, T_p(E)) \to H^1_{/S}(\mathbb{Q}_{n,p}, T_p(E)),$$

*where the first arrow is the localization and the second is the natural projection. Then*

$$\sigma(\sum_{\gamma \in \Gamma_n} \chi(\gamma) \exp^*_{\omega_E}(\mathrm{loc}_p^{ram}(c_n^\gamma))) = \frac{r_E}{\Omega_E} L_{(pN_E)}(E, \chi, 1),$$

*for any character $\chi$ of $\Gamma_n$. Here $r_E$ is a positive integer which depends only on $E$ and $\Omega_E$ is the fundamental real period. $L_{(pN_E)}(E, \chi, s)$ is a function obtained from $L(E, \chi, s)$ removing Euler factors at primes which divide $pN_E$.*

Let

$$\kappa_n = \sum_{\gamma \in \Gamma_n} \exp^*_{\omega_E}(\mathrm{loc}_p^{ram}(c_n^\gamma))\gamma \in \mathbb{C}_p[\Gamma_n].$$

Then $\{\kappa_n\}_n$ forms a projective system by **Fact 2.2** and

$$\chi(\sigma(\phi(\kappa_\infty))) = \frac{r_E}{\Omega_E} L_{(pN_E)}(E, \chi^{p-1}, 1), \quad \kappa_\infty = \lim_{\leftarrow} \kappa_n,$$

for any finite character $\chi$ of $\Gamma_\infty$ by **Lemma 2.3**. Since

$$L_{(pN_E)}(E, \chi, 1) = \prod_{q|pN_E} P_q(q^{-1}\chi(\mathrm{Fr}_q))L(E, \chi, 1),$$

where

$$P_q(t) = \begin{cases} 1-t, & \text{if } E \text{ has a split multiplicative reduction at } q: \\ 1+t, & \text{if } E \text{ has a non-split multiplicative reduction at } q: \\ 1, & \text{if } E \text{ has an additive reduction at } q, \end{cases}$$

**Theorem 2.1** implies the following result.

**Proposition 2.6.**

$$\sigma(\phi(\kappa_\infty)) = \frac{r_E}{\Omega_E} \prod_{q|N_E, q\neq p} \phi(P_q(q^{-1}\mathrm{Fr}_q) \cdot \mu_{E,\infty}).$$

2.4. **A motivation of the conjecture.** Now we are ready to explain a motivation of **Conjecture 1.1**. We will fix a positive integer $b$ greater than 1 which is prime to $p$ and set $a = b^{p-1}$. In order to make a distinction between $p$-adic and archimedian logarithm of $a$ we denote them by $l_p(a) \in \mathbb{C}_p$ and $l_\infty(a) \in \mathbb{C}$, respectively. We refer an isomorphism $\sigma : \mathbb{C}_p \to \mathbb{C}$ is *normalized* if it satisfies

(1)

$$\sigma(z) = z, \quad z \in \bar{\mathbb{Q}}.$$

(2)

$$\sigma(l_p(a)) = l_\infty(a).$$

Let us extends $\sigma$ to $\mathbb{C}_p[[s]]$ and $\mathbb{C}_p[[X_a]]$ by

$$\sigma(\sum_n c_n s^n) = \sum_n (c_n) s^n,$$

and

$$\sigma(\sum_n d_n X_a^n) = \sum_n \sigma(d_n) X_a^n.$$

Then (2) implies

$$\sigma(a^{-s}) = a^{-s},$$

as a power series of $s$ and in particular

$$\sigma \circ \hat{\tau}_p = \hat{\tau}_\infty \circ \sigma. \tag{10}$$

Finally we define

$$\sigma : \mathbb{C}_p[[\Gamma_\infty]] \to \mathbb{C}[[\Gamma_\infty]]$$

to be the inverse limit of

$$\sigma : \mathbb{C}_p[\Gamma_r] \to \mathbb{C}[\Gamma_r], \quad \sigma(\sum_{\gamma \in \Gamma_r} c_\gamma \gamma) = \sum_{\gamma \in \Gamma_r} \sigma(c_\gamma)\gamma.$$

Since $\sigma$ is normalized,

$$\sigma(\chi(c)) = \chi(\sigma(c)), \quad c \in \mathbb{C}_p[[\Gamma_\infty]],$$

for a finite character $\chi$ of $\Gamma_\infty$. Let $\Lambda$ be a $\mathbb{C}$-subalgebra of $\mathbb{C}[[\Gamma_\infty]]$ generated by $\sigma(\Lambda_{\mathbb{C}_p})$ and $\Lambda_{\mathbb{C}}$ and $\mathfrak{M}_\Lambda$ the intersection of it and the argumentation ideal of $\mathbb{C}[[\Gamma_\infty]]$. Then $\Lambda$ contains $\mathbb{C}[X_a]$ and

$$\Lambda/\mathfrak{M}_\Lambda^r = \mathbb{C}[X_a]/(X_a)^r \overset{\hat{\tau}_\infty}{\simeq} \mathbb{C}[[s]]/(s^r), \quad \forall r \tag{11}$$

by **Proposition 2.1** and **Proposition 2.4**. Therefore we see that, for $\lambda \in \Lambda$,

$$\mathrm{Min}\{k \mid \lambda \in \mathfrak{M}_\Lambda^k\} = \mathrm{ord}_{s=0}\hat{\tau}_\infty(\lambda). \tag{12}$$

Let $E$ and $E'$ be elliptic curves satisfying the assumption of **Conjecture 1.1**. By **Proposition 2.2** and **Theorem 2.1** we see that

$$\frac{\phi(\mu_{E',\infty})}{\Omega_{E'}} \cdot \sigma(\iota\phi(\mu_{E,p})) = \frac{\phi(\mu_{E,\infty})}{\Omega_E} \cdot \sigma(\iota\phi(\mu_{E',p})) \in \Lambda. \tag{13}$$

Now **Conjecutre 1.1** will be derived by (10), (12), **Proposition 2.2** and **Theorem 2.1**.

Unfortunately there seems to be a mistake in the above argument. In fact suppose that both $E$ and $E'$ have a split multiplicative reduction at $p$ and that their L-function does not vanish at $s = 1$. Take the image of (13) by $\hat{\tau}_\infty$ and the formula of the first derivative of $p$-adic L-function ([2], [5]) will tell us that their L-invariants should be equal! Since we cannot solve this puzzle the above argument should be considered as only an explanation and not a proof. But suppose that $E'$ is a quadratic twist of $E$ (as we will see in the next section, in order to derive consequences from **Conjecture 1.1**, we may impose this). Because they are isomorphic over $\overline{\mathbb{Q}}$ their $j$-invariants are equal and so are L-invariants since the Tate period is determined by the $j$-invariant ([7] **Chapter II** $1 (2)).

**Conjecture 2.1.** *Let $E$ and $E'$ be elliptic curves defined over $\mathbb{Q}$. Suppose that $E'$ is a quadratic twist of $E$ and that they have ordinary reduction of the same type at $p$. Then*

$$\Omega_{E'} L(E, 1-s)\sigma(\mathcal{L}_{E',p}(s)) = \Omega_E L(E', 1-s)\sigma(\mathcal{L}_{E,p}(s)).$$

Although our argument may be incomplete it will explain why an extra zero appears. We will follow the notation of [11] **Appendix**. Suppose that $E$ has a split multiplicative reduction at $p$. For simplicity we will omit to write the isomorphism $\sigma : \mathbb{C}_p \to \mathbb{C}$ and will make no distinction between $\hat{\tau}_p$ and $\hat{\tau}_\infty$, which will be denoted by $\hat{\tau}$. Let us put

$$x_n = \mathrm{Tr}_{\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}_{n,p}}(\sum_{k=0}^{n} \frac{\zeta_{p^{n+1-k}} - 1}{p^k} + \frac{p}{p-1}) \in \mathbb{Q}_{n,p}$$

and

$$w_n = \sum_{\gamma \in \Gamma_n} x_n^\gamma \gamma \in \mathbb{Q}_{n,p}[\Gamma_n].$$

One may check that $\{x_n\}_n$ is compatible with the corestrictions and that $\{w_n\}_n$ forms a projective system. According to Coleman define

$$\mathrm{Col}_n(\kappa_n) := w_n \iota(\kappa_n) = \sum_{\gamma \in \Gamma_n} (\mathrm{Tr}_{\mathbb{Q}_{n,p}/\mathbb{Q}_p} x_n^\gamma) \exp^*_{\omega_E}(\mathrm{loc}_p^{ram}(c_n))\gamma^{-1}.$$

It is known that it is contained in $\mathbb{Z}_p[\Gamma_n]$ and that ([11] **Corollary 7.2**)

$$r_E \prod_{q|N_E, q\neq p} P_q(q^{s-1})\mathcal{L}_{E,p}(s) = \hat{\tau}(\mathrm{Col}_\infty(\kappa_\infty)), \quad \mathrm{Col}_\infty(\kappa_\infty) = \varprojlim \mathrm{Col}_n(\kappa_n).$$

Therefore

$$r_E \prod_{q|N_E, q\neq p} P_q(q^{(p-1)s-1})\mathcal{L}_{E,p}((p-1)s) = \hat{\tau}\phi(\mathrm{Col}_\infty(\kappa_\infty)).$$

Since $\mathrm{Col}_\infty(\kappa_\infty) = w_\infty \iota(\kappa_\infty)$ we formally obtain

$$r_E \prod_{q|N_E, q\neq p} P_q(q^{(p-1)s-1})\mathcal{L}_{E,p}((p-1)s) = \hat{\tau}(\phi(w_\infty)) \cdot \hat{\tau}(\iota\phi(\kappa_\infty)).$$

By **Theorem 2.1** and **Proposition 2.6** the second term is

$$\hat{\tau}(\iota\phi(\kappa_\infty)) = \frac{r_E}{\Omega_E} \prod_{q|N_E, q\neq p} P_q(q^{(p-1)s-1})L^\dagger(E, 1-(p-1)s).$$

and therefore

$$\mathcal{L}_{E,p}((p-1)s) = \hat{\tau}(\phi(w_\infty))\frac{L^\dagger(E, 1-(p-1)s)}{\Omega_E}.$$

But what $\hat{\tau}(\phi(w_\infty))$ should be? By [11] **Lemma A.1 (2)** we know that

$$\chi(w_\infty) = \begin{cases} W(\chi), & \text{if } \chi \text{ is nontrivial} \\ 0, & \text{if } \chi \text{ is trivial.} \end{cases}$$

Now remember that $W(\chi)$ appears in the functional equation of Dirichlet series:

$$L(0,\chi) = \frac{1}{\pi i} W(\chi) L(1, \chi^{-1}).$$

If we were able to replace $\chi$ by $\chi_s$ as the introduction it would be

$$\zeta_{(p)}(s) = \frac{1}{\pi i}\hat{\tau}(\sigma(w_\infty))\zeta_{(p)}(1-s),$$

where $\zeta_{(p)}(s) = (1-p^{-s})\zeta(s)$. In particular

$$\hat{\tau}(\phi(w_\infty)) = \frac{\pi i \zeta_{(p)}((p-1)s)}{\zeta_{(p)}(1-(p-1)s)},$$

and since the zeta function has a simple pole at $s = 1$ the order of $\hat{\tau}_\infty(\phi(w_\infty))$ at $s = 0$ is one.

## 3. Consequences of the conjecture

3.1. **An application to Mazur-Tate-Teitelbaum conjecture.** Let $E$ be an elliptic curve defined over $\mathbb{Q}$. The following conjecture is due to Mazur, Tate and Teitelbaum.

**Conjecture 3.1.** (1) *Suppose that $E$ has an good ordinary or a non-split multiplicative reduction at $p$. Then*

$$\mathrm{ord}_{s=0}\mathcal{L}_{E,p}(s) = \mathrm{ord}_{s=1}L(E,s).$$

(2) *Suppose that $E$ has split multiplicative reduction at $p$. Then*

$$\mathrm{ord}_{s=0}\mathcal{L}_{E,p}(s) = 1 + \mathrm{ord}_{s=1}L(E,s).$$

Suppose that $L(E,1) \neq 0$. If $E$ has a good ordinary or a non-split multiplicative reduction at $p$ the conjecture is trivially true by **Fact 2.1**. If $E$ has a split multiplicative reduction it has been proved by Greenberg and Stevens [2]. Later Kobayashi gives an elementary proof of their statements using Kato's result [5]. Obviously our conjecture follows from **Conjecture 3.1**. Conversely, using a theorem due to Ono and Skinner [8], we will show that **Conjecture 1.1** implies **Conjecture 3.1**.

Let $\Pi = \{p_1, \cdots, p_t\}$ be a set of mutually distinct primes and take $\epsilon = (\epsilon_1, \cdots \epsilon_t)$ where $\epsilon_i \in \{\pm 1\}$. Then we define $P(\Pi, \epsilon)$ to be a set of square free fundamental discriminants $D$ which satisfy

$$(\frac{D}{p_i}) = \epsilon_i, \quad \forall i,$$

where $(\dot{\cdot})$ denotes Legendre symbol. For a square free fundamental discriminant $D$ let $E_D$ be the twist of $E$ over $\mathbb{Q}(\sqrt{D})$. Namely if

$$E \,:\, y^2 = x^3 - ax + b, \quad a, b \in \mathbb{Q},$$

is a Weierstrauss form of $E$, $E_D$ is defined to be

$$E_D \,:\, Dy^2 = x^3 - ax + b.$$

**Fact 3.1.** *(*[8] **Corollary 3***) For a positive number $X$*

$$\sharp\{D \in P(\Pi, \epsilon) \,:\, |D| < X,\, L(E_D, 1) \neq 0\} >> \frac{X}{\log X}.$$

.

**Proof of Conjecture 1.1 ⇒ Conjecture 3.1.** By **Fact 3.1** we know that there is a square free fundamental discriminant $D$ satisfying $(\frac{D}{p}) = 1$ and $L(E_D, 1) \neq 0$. The first condition guarantees that $E$ and $E_D$ have ordinary reduction of the same type at $p$. As we have mentioned before the conjecture is true for $E_D$ and **Conjecture 3.1** is derived from **Conjecture 1.1**.

3.2. **A review of Iwasawa theory for an elliptic curve.** Let $E$ be an elliptic curve defined over $\mathbb{Q}$ with good ordinary reduction at a prime $p \geq 5$. We denote the Selmer group of $E$ over $\mathbb{Q}_n$ by $\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])$ and define

$$\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty]) := \varinjlim \mathrm{Sel}(\mathbb{Q}_n, E[p^\infty]),$$

where limits with respect to restrictions. In general let $M$ be a profinite $\mathbb{Z}_p$-module. Its $p$-adic and rational $p$-adic Pontryagin dual is define to be

$$\mathbb{D}(M) := \mathrm{Hom}_{conti}(M, \mathbb{Q}_p/\mathbb{Z}_p),$$

and

$$\mathbb{D}^0(M) := \mathbb{D}(M) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,$$

respectively. The subscript *conti* means the set of continuous homomorphisms. By $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]] \simeq \mathbb{Z}_p[[t]]$, we regard $X_\infty := \mathbb{D}(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty]))$ as a $\mathbb{Z}_p[[t]]$-module. It is known that $X_\infty$ is a torsion $\mathbb{Z}_p[[t]]$-module and therefore $\mathbb{D}^0(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty]))$ is a torsion $\Lambda_{\mathbb{Q}_p}$-module. Here we put $\Lambda_{\mathbb{Q}_p} := \mathbb{Z}_p[[t]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, which is a discrete valuation ring whose valuation ideal is generated by $t$. Let $\mathrm{Char}(X_\infty) \subset \Lambda_{\mathbb{Q}_p}$ be the characteristic ideal of $\mathbb{D}^0(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty]))$ and the order of its generator with respect to $t$ is denoted by $\mathrm{ord}_t\mathrm{Char}(X_\infty)$.

**Proposition 3.1.**

$$\mathbb{D}^0(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty]))^{\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})} \simeq \mathbb{D}^0(\mathrm{Sel}(\mathbb{Q}, E[p^\infty])).$$

**Proof.** Immediate from [9] **Lemme 6.6**.□

Let $\text{Ш}(E/\mathbb{Q})$ be the Shafarevich-Tate group. Taking rational $p$-adic Pontryagin dual of

$$0 \to E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}(\mathbb{Q}, E[p^\infty]) \to \text{Ш}(E/\mathbb{Q})[p^\infty] \to 0,$$

we have

$$0 \to \mathbb{D}^0(\text{Ш}(E/\mathbb{Q})[p^\infty]) \to \mathbb{D}^0(\mathrm{Sel}(\mathbb{Q}, E[p^\infty])) \to \mathrm{Hom}_{\mathbb{Z}}(E(\mathbb{Q}), \mathbb{Z}) \otimes \mathbb{Q}_p \to 0.$$

**Propositon 3.1** implies the following theorem.

**Theorem 3.1.**

$$\mathrm{ord}_t\mathrm{Char}(X_\infty) \geq \mathrm{rank}E(\mathbb{Q}).$$

*Moreover if* $\text{Ш}(E/\mathbb{Q})[p^\infty]$ *is finite the equality holds.*

3.3. **Birch and Swinnerton-Dyer conjecture for a semistable elliptic curve.**

**Lemma 3.1.** *Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and $L$ be a quadratic extension of $\mathbb{Q}$. Then for any odd prime $p$ and a positive integer $r$ the restriction gives an isomorphism,*

$$\text{Ш}(E/\mathbb{Q})[p^r] \simeq \text{Ш}(E/L)[p^r].$$

**Proof.** Since $p$ is odd and since the order of $\mathrm{Gal}(L/\mathbb{Q})$ is two, $H^1(\mathrm{Gal}(L/\mathbb{Q}), E(L))[p^r] = H^2(\mathrm{Gal}(L/\mathbb{Q}), E(L))[p^r] = 0$. Therefore the inflation-restriction sequence implies

$$H^1(\mathbb{Q}, E)[p^r] \simeq H^1(L, E)[p^r].$$

Let $v$ be a place (including $\infty$) of $\mathbb{Q}$. Suppose that $v$ ramifies or inerts in $L$ and let $w$ be the place of $L$ over $v$. The same argument as above shows

$$H^1(\mathbb{Q}_v, E)[p^r] \simeq H^1(L_w, E)[p^r].$$

Suppose $v$ splits in $L$ and let $w$ and $w'$ be places of $L$ over $v$. Then both $L_w$ and $L_{w'}$ are isomorphic to $\mathbb{Q}_v$ and

$$H^1(\mathbb{Q}_v, E)[p^r] \overset{\text{Res}}{\to} H^1(L_w, E)[p^r] \times H^1(L_{w'}, E)[p^r],$$

is the diagonal imbedding,

$$H^1(\mathbb{Q}_v, E)[p^r] \overset{\Delta}{\to} H^1(\mathbb{Q}_v, E)[p^r] \times H^1(\mathbb{Q}_v, E)[p^r].$$

Thus we find that $g$ (reps. $h$) of

$$\begin{tikzcd}
0 \arrow[r] \arrow[d] & Ш(E/\mathbb{Q})[p^r] \arrow[r] \arrow[d, "f"'] & H^1(\mathbb{Q}, E)[p^r] \arrow[r] \arrow[d, "g"'] & \prod_v H^1(\mathbb{Q}_v, E)[p^r] \arrow[d, "h"'] \\
0 \arrow[r] & Ш(E/L)[p^r] \arrow[r] & H^1(L, E)[p^r] \arrow[r] & \prod_w H^1(L_w, E)[p^r],
\end{tikzcd}$$

is isomorphic (resp. injective). A simple diagram chasing shows that $f$ is an isomorphism. □

**Proposition 3.2.** *Let $E$ be an semi-stable elliptic curve defined over $\mathbb{Q}$. Then there is a pair $(D, p)$ such that*

(1) *$D$ is a square free fundamental discriminant so that*

$$L(E_D, 1) \neq 0.$$

(2) *$p$ is a good ordinary prime of $E$ which satisfies*

$$(\frac{D}{p}) = 1, \quad Ш(E_D/\mathbb{Q})[p] = 0, \quad p \geq 11.$$

**Proof.** By **Fact 3.1** there is a fundamental discriminant satisfying (1). Let us fix one of them. Then by [4] we know that $Ш(E_D/\mathbb{Q})$ is a finite abelian group. Since $E$ is semistable it does not have complex multiplication and, due to Serre, the density of supersingular primes of $E$ is 0. Therefore there is a prime satisfying (2). □

The following theorem is a direct consequence of [14] **Corollary 3.6.10**.

**Theorem 3.2.** *Let $E$ be a semistable elliptic curve defined over $\mathbb{Q}$. Let $p \geq 11$ be a prime where $E$ has good ordinary reduction. Then*

$$\mathrm{ord}_t \mathrm{Char}(X_\infty) = \mathrm{ord}_{s=0} \mathcal{L}_{E,p}(s).$$

**Theorem 3.3.** *Let $E$ be a semistable elliptic curve defined over $\mathbb{Q}$. Then we have the following consequences.*

(1) *The rank of $E(\mathbb{Q})$ is equal to $\mathrm{ord}_{s=1} L(E, s)$.*
(2) *For an odd prime $q$ the $q$-primary part $Ш(E/\mathbb{Q})[q^\infty]$ of the Shafarevich-Tate group of $E$ over $\mathbb{Q}$ is finite. Moreover it is trivial except finitely many primes.*

**Proof.** Let $(D,p)$ be a pair of **Proposition 3.2**. Since $p$ is a good ordinary prime of $E$ and since $(\frac{D}{p})=1$, $E$ and $E_D$ have a good ordinary reduction of the same type at $p$. By $L(E_D,1)\neq 0$, **Fact 2.1** shows that the order of $p$-adic L-function of $E_D$ at the origin is zero. Then by **Conjecture 1.1** and **Theorem 3.2**,

$$\mathrm{ord}_{s=1}L(E,s)=\mathrm{ord}_t\mathrm{Char}(X_\infty). \tag{14}$$

On the other hand since $E$ and $E_D$ are isomorphic over $\mathbb{Q}(\sqrt{D})$, by **Lemma 3.1**,

$$Ш(E/\mathbb{Q})[q^r]\simeq Ш(E/\mathbb{Q}(\sqrt{D}))[q^r]\simeq Ш(E_D/\mathbb{Q})[q^r], \tag{15}$$

for any odd prime $q$ and a positive integer $r$. In particular since $Ш(E_D/\mathbb{Q})[p]=0$ we see $Ш(E/\mathbb{Q})[p]=0$. Now **Theorem 3.1** and (14) implies

$$\mathrm{ord}_{s=1}L(E,s)=\mathrm{rank}E(\mathbb{Q}).$$

Kato has shown that $L(E_D,1)\neq 0$ implies finiteness of $Ш(E_D/\mathbb{Q})$([4]). Thus (15) shows that $Ш(E/\mathbb{Q})[q^\infty]$ is finite for an odd prime $q$ and moreover vanishes except finitely many primes. □

3.4. **Birch and Swinnerton-Dyer conjecture for an elliptic curve defined with a complex multiplication.** Let $E$ be an elliptic curve defined over $\mathbb{Q}$ whose endomorphism ring is isomorphic to the integer ring $\mathcal{O}_K$ of a quadratic imaginary field $K$. Then the following is a direct consequence of [10]**Theorem 12.3**.

**Theorem 3.4.** *Let $p\geq 5$ be a prime where $E$ has good ordinary reduction. Then*

$$\mathrm{ord}_t\mathrm{Char}(X_\infty)=\mathrm{ord}_{s=0}\mathcal{L}_{E,p}(s).$$

**Theorem 3.5.** *Let $E$ be an elliptic curve defined over $\mathbb{Q}$ whose endomorphism ring is isomorphic to $\mathcal{O}_K$. Then we have the following consequences.*

1. *The rank of $E(\mathbb{Q})$ is equal to $\mathrm{ord}_{s=1}L(E,s)$.*
2. *For an odd prime $q$ the $q$-primary part $Ш(E/\mathbb{Q})[q^\infty]$ of the Shafarevich-Tate group of $E$ over $\mathbb{Q}$ is finite. Moreover it is trivial except finitely many primes.*

**Proof.** Let $d_K$ be the discriminant of $K$ and $d_K=q_1^{e_1}\cdots q_t^{e_t}$ be its factorization by primes. We choose an odd prime $l$ such that $(\frac{d_K}{l})=1$. By **Fact 3.1** there is a square free fundamental discriminant $D$ satisfying

$$(\frac{D}{q_1})=\cdots(\frac{D}{q_t})=(\frac{D}{l})=1,$$

and $L(E_D,1)\neq 0$. Note that the condition of $\{q_i\}_i$ implies that $d_K$ and $D$ are coprime. Let $R$ be a multiplicative closed set consisting of $\{-1,0,1\}\subset\mathbb{Z}$ and consider a multiplicative map:

$$\mathbb{Z}/(d_K)\times\mathbb{Z}/(D)\overset{\chi}{\to}R\times R,\quad \chi(x,y)=((\frac{d_K}{x}),(\frac{D}{y})),$$

which may be regarded as a map from $\mathbb{Z}/(d_KD)$. Since $\chi(l)=(1,1)$ there are infinitely many primes $q$ satisfying $\chi(q)=(1,1)$ ( In fact it is sufficient that $q\equiv l \pmod{d_KD}$). On the other hand since $L(E_D, 1) \neq 0$, $Ш(E_D/\mathbb{Q})$ is a finite group [10]. Therefore there is an odd prime $p$ which does not divide the discriminant of $E$ and satisfies

$$Ш(E_D/\mathbb{Q})[p] = 0, \quad (\frac{d_K}{p}) = (\frac{D}{p}) = 1.$$

The last condition gurantees that $E$ has good ordinary reduction at $p$ and that $E$ and $E_D$ are of same type at $p$. Now the remaining of a proof is the same as one of **Theorem 3.3** (One uses **Theorem 3.4** in stead of **Theorem 3.2**). □

## References

[1] C. Breuil, B. Conrad, F. Diamond and R. Taylor. On the modularity of elliptic curves over $\mathbb{Q}$ : Wild 3-adic exercises. *Journal of American Mathematical Society*, 14, 4:843–939, 2001.

[2] R. Greenberg and G. Stevens. $p$-adic $L$-functions and $p$-adic periods of modular forms. *Inventiones Mathematicae*, 111, 2:407–447, 1993.

[3] H. Hida. Elementary theory of $L$-functions and Eisenstein series. *Cambridge University Press, London Mathematical Society Student Texts* 26, 1993.

[4] K. Kato. $p$-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:117-290, 2004.

[5] S. Kobayashi. An elementary proof of Mazur-Tate-Teitelbaum conjecture for elliptic curves. *Documenta Mathematica.*, Extra Volume Coates:567–576, 2006.

[6] B. Mazur and P. Swinnerton-Dyer. Arithmetic of Weil curves. *Inventiones Mathematicae*, 25:1–61, 1974.

[7] B. Mazur, J. Tate and J. Teitelbaum. On $p$-adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Inventiones Mathematicae*, 84:1–48, 1986.

[8] K. Ono and C. Skinner. Non-vanishing of quadratic twists of modular L-functions. *Inventiones Mathematicae*, 134:651–660, 1998.

[9] B. Perrin-Riou. Théorie d'Iwasawa $p$-adique locale et globale. *Inventiones Mathematicae*, 99:247–292, 1990.

[10] K. Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Inventiones Mathematicae*, 103: 25-68, 1991.

[11] K. Rubin. Euler Systems and modular elliptic curves. in *Galois Representations in Arithmetic Algebraic Geometry, London Mathematical Society*, 254, 1998.

[12] K. Rubin. Euler Systems. *Annals of Mathematical Studies*, 147, 2000.

[13] J. H. Silverman. The Arithmetic of Elliptic Curves. *Springer GTM*, 106, 1986.

[14] C. Skinner and E. Urban. The Iwasawa main conjectures for $GL_2$. *Preprint.*

[15] L. C. Washington. Introduction to Cyclotomic Fields. *Springer GTM*, 83, 1997.

[16] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Annals of Mathematics*, 141:443–551, 1995.